BAB II

DASAR TEORI

2.1 Konsep Jaringan

Jaringan merupakan efek dari perkembangan teknologi dalam aspek pertukaran informasi baik dalam skala area kecil maupun area yang sangat luas. Jaringan dalam perkembangannya dapat menggunakan jaringan *wireless* maupun menggunakan LAN yang dalam aplikasinya dapat ditemui pada perkantoran, rumah, kampus, dll. Pada penggunaan *wireless* dan LAN masing-masing memiliki kelebihan dan kekurangannya yang digunakan pada suatu jaringan sebagai berikut:

1. Dapat Menghemat Biaya.

   Dalam segi biaya dapat menekan kebutuhan biaya yang dikeluarkan misal pada jaringan LAN dapat menggunakan satu perangkat printer yang terhubung dalam satu jaringan yang sama.

2. Mempercepat proses sharing data (berbagi data)

   Dalam pertukaran data dijaringan yang sudah *share* maka lebih cepat dari pada menggunakan jaringan *wireless* sdengan proses yang cenderung stabil.

3. Menjaga informasi agar tetap up-to-date dan andal

   Dengan konfigurasi yang tepat maka data juga dapat diakses dari luar dengan ketentuan memiliki koneksi internet.

2.2 Internet Protocol Address

Jaringan yang telah dikonfigurasi membutuhkan IP yang merupakan alamat pada jaringan perangkat komputer yang nantinya dikonfigurasikan untuk dapat melakukan komunikasi antar perangkat komputer baik jaringan lokal

maupun jaringan internet. Pada aplikasinya IP dapat diatur menjadi dinamik maupun statik dan penggunaannya sesuai dengan desain atau kebutuhan.

Pada perangkat yang telah diatur IP berarti perangkat tersebut dianggap memiliki alamat untuk mengirim atau menerima paket data. Hal ini seperti diilustrasikan jika kita ingin mengirimkan surat melalui jasa kantor pos dimana baik kedua belah pihak harus memiliki alamat yang jelas agar surat yang dikirim dapat diterima oleh pengirim dengan keadaan utuh. Konsep penggunaan IP hampir sama seperti ilustrasi tersebut dimana pengalamatan IP telah diterima diseluruh dunia dan terdapat standart yang harus dipenuhi. Dengan memberikan IP pada perangkat komputer yang dikenal dengan ethernet maka komputer tersebut telah memiliki alamat untuk dituju,

Pada konsep IP yang digunakan terdiri dari 32bit bilangan biner yang dipisahkan dengan titik disetiap 8bit. Penggunaan notasi pada IP jarang digunakan dan banyak menggunakan bilangan desimal dengan 4 bilangan yang masing-masing dipisahkan oleh 4 buat titik yang mana lebih dikenal dengan “notasi desimal bertitik”. Setiap bilangan decimal merupakan nilai dari satu oktet *IP address*.

Aplikasi IP pada komputer memiliki garis pemisah antar bagian network ataupun *host* dimana penggunaan IP juga memiliki aturan yang telah ditetapkan seperti penggunaan IP sesuai dengan kelas yaitu A, B, C, D. Perbedaan kelas IP terletak pada ukuran dan jumlah penggunaan IP pada *host.* Sehingga pengaruh ukuran tersebut penggunaan kelas menyesuaikan dengan kebutuhan jaringan yang ingin didesain.

2.3 Internet Protocol-Security

Penggunaan *Internet Protocol Security* pada suatu jaringan sangat memberikan dampak yang baik dimana memberikan keamanan saat proses pengiriman paket data terjadi. Keamanan jaringan pada IPSec merupakan keamanan dengan konsep kriptografi untuk IPv4 dan IPv6 yang bekerja pada lapisan *network*, melakukan proteksi dan melakukan otentikasi komunikasi pada IP antar *host* dengan konfigurasi yang tepat shingga memberikan fungsi yang pada laju lalulintas data padda IPv4 dan IPv6[7]. *IP Sec* sebenarnya adalah fitur yang dimiliki oleh IPv6 namun oleh beberapa developer diaplikasikan ke dalam IPv4. Pada layanan IPSec yang banyak digunakan meliputi integritas, kontrol akses autentikasi data, proteksi, dan enskripsi proses dan memiliki pembatasan lalu lintas data yang terjadi. Layanan yang tersedia termasuk fasilitas yang ada dalam IP layer dan dapat memberikan perlindungan pada IP yang telah di konfigurasi. Tidak hanya itu IPsec Key Exchange and Management Protocol (ISAKMP) untuk manajemen kunci yang menentukan negosiasi, pembentukan, perubahan, dan penghilangan asosiasi keamanan[8]. Pada tujuan penggunaan IPSec untuk mengamankan data yang akan dikirim dengan jalur pengamanan melalui protokol manajmen basis kriptografi. Pada konfigurasi yang dilakukan dimana pada masing-masing IP jaringan yang telah diatur untuk memiliki keamanan maka perlu dibutuhkan algorith yang dipakai seperti penggunaan MD5 dengan authentikasi yang sama.

Pada standart yang telah dibuat oleh IETF yaitu memanfaatkan mekanisme kriptografi pada lapisan jaringan sehingga pada setiap aktifitas pengiriman paket data harus memiliki autentikasi, verifikasi integritas paket data, dan menjada kerahasiaan muatan dari paket data. Dimana data-data tersebut di enskrips untuk

memenuhi dari standart tersebut dan memiliki dukungan pertukaran informasi antar paket yang aman melalui IP layer.

2.3.1. Protokol Layanan Keamanan IP-Sec

IPSec menggunakan dua protokol untuk menyediakan layanan keamanan lalu lintas yaitu Authentication Header (AH) and Encapsulating Security Payload (ESP) . Dalam mode tunnel, header IPSec (header AH atau ESP) disisipkan di antara header IP dan protokol lapisan atas. Antara AH dan ESP, ESP paling umum digunakan dalam konfigurasi Tunnel VPN IPSec[9]. Berikut merupakan implementasi dari IPSec yang harus mendukung dengan ESP dan juga AH:

1. Pada penggunaan protokol AH harus menyediakan integritas, autentikasi dan keamanan layanan.
2. Penggunaan pada protokol ESP harus dapat merahasikan data yang dikirim dan pembatasan aliran lalu lintas kerahasiaan.
3. Pada kedua protokol diatas digunakan untuk kontrol akses dengan basis kroptografi dan memanajemen keamanan pada protokol keamanan dari layanan.

2.4 Software Defined Wide Area Network

Seperti penjelasan pada pendahuluan terkait dengan SD-WAN yang merupakan perkembangan tekonologi dengan dasar teknologi SDN yang merupakan teknologi baru yang banyak digunakan pada jaringan perkantoran dan memiliki data pusat dengan letak geografis yang luas. Teknologi ini sangat membantu meringankan erjadinya kesalahan khususnya pada *human error* yang banyak terjadi.

Adalah bentuk aplikasi spesifik dari teknologi *software-defined networking* (SDN) yang diaplikasikan pada koneksi WAN (*wide area network*), yang digunakan untuk menghubungkan jaringan perusahaan termasuk kantor-kantor cabang dan *data center* yang memiliki jarak geografis luas. Teknologi ini akan membantu meringankan kompleksitas dengan *zero touch provisioning* yang mampu mengatasi resiko *human error*.

Secara teknis, SD-WAN memiliki perbedaan dengan WAN secara sistem lama dimana cara kerjanya hanya melalui menyalurkan layanan IP ke klien yang dituju. Hal ini dilakukan melalui *hardware* yang mendasarinya untuk melengkapi jaringan secara keseluruhan. Cakupan dari beberapa jenis jaringan ini membutuhkanupaya yang rumit bagi tim IT karena jumlah *hardware* yang dipasang dan proses yang diperlukan dalam mengelola aktivitas jaringan. Lain halnya dengan SD-WAN yang memanfaatkan solusi *tunneling* pada arsitektur jaringan yang sudah ada sebelumnya. SD-WAN menyederhanakan manajemen dan operasi WAN dengan memisahkan perangkat keras jaringan dari mekanisme kontrolnya. SD-WAN memberi perusahaan opsi untuk secara dinamis menghubungkan jaringan kantor cabang dan kantor pusat misalnya, dengan memanfaatkan kemampuan Internet dan *cloud* bersama. Ada banyak manfaat dari SD-WAN yang mampu membantu jaringan pada bisnis Anda menjadi lebih praktis dibanding penggunaan WAN tradisional. Berikut 5 Hal tentang SD-WAN yang perlu Anda ketahui.

1. Performansi

   Perbedaan SD-WAN dan WAN tradisional yang paling terasa adalah peningkatan performansi. Pada WAN,waktu *failover* tergantung seberapa cepat perubahan *routing* pada *router*.

2. Waktu

   Penggunaan WAN tradisional ketika perusahaan membuat jaringan baru di kantor cabang akan memakan waktu. Meski secara umum durasinya hampir sama, instalasi SD-WAN bisa dilakukan lebih cepat berkat teknologi Zero Touch Provision. *Failover time* saat ada perpindahan dari satu *link* ke *link* lainnya pun menjadi hampir tidak terasa dengan dukungan teknologi Link Steering/Dynamic Multipath Optimization (DMPO).

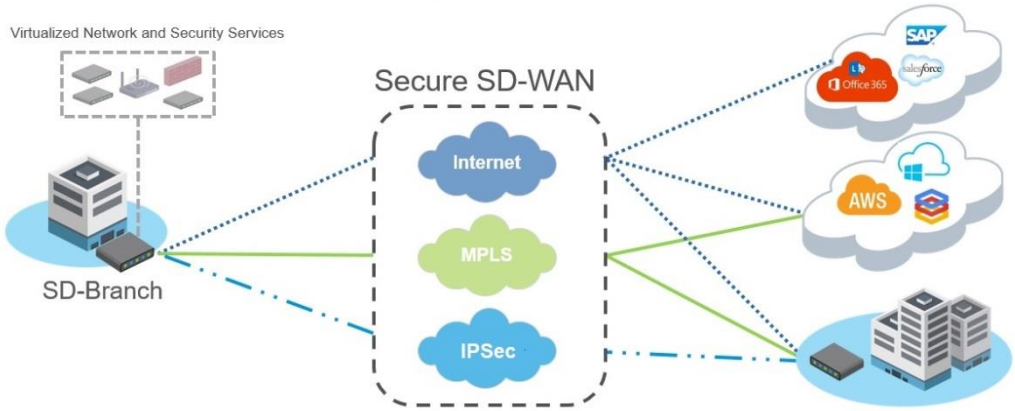
3. Fleksibilitas

   WAN tradisional sangat bergantung pada *data center*. Ini mengharuskan lalu lintas jaringan di-*backhaul* melalui *data center* sehingga bisa tersumbat. Sementara itu SD-WAN memiliki kumpulan *bandwith* terpadu yang disediakan oleh beberapa penyedia layanan. Hal ini memungkinkan pemanfaatan sumber daya jaringan yang lebih besar ketika data bermigrasi di lintas kantor.

   Kapasitas koneksi *Data center* yang menjadi tumpuan WAN tradisional memiliki keterbatasan kapasitas. Khususnya untuk menangani koneksi yang masuk ke beberapa *platform cloud*. Hal ini tidak akan terjadi pada SD-WAN karena tidak dibatasi dengan *hardware* yang mengakomodir jaringan

4. Konfigurasi

   Kebijakan konfigurasi perangkat pendukung WAN tradisional harus dilakukan secara mandiri, sesuai dengan basis per perangkat. Hal ini dilakukan agar konfigurasi bisa diterapkan dengan baik. Di SD-WAN, aplikasi WAN diprioritaskan secara menyeluruh. Selain itu, perusahaan bisa memantau lalu lintas secara *real-time* saat terjadi *brownout*.



Gambar 2.1 IllustrasiSistem SD-WAN

2.5 Penelitian Sebelumnya

Penelitian sebelumnya yang telah dituangkan pada latar belakang dimana sistem yang dirancangan menggunakan jaringan VPN walau menggunakan keamanan dengan tunneling *IPSec* sebagai tambahan keamanan saat proses pengiriman data yang akan dikirim. Selain itu pada penelitian Herry Prasetyo Nugroho dengan judul "Desain Dan Manajemen Jaringan Komputer Fakultas Teknik Universitas Muhammadiyah Malang (UMM) Berbasis *Software Defined Networking* (SDN) juga dijelaskan penggunaan SDN-WAN pada jaringan dilingkungan kampus tetapi lebih fokus pada penggunaan SDN itu sendiri tanpa adanya pengamanan tambahan seperti menggunakan IPSec. Dapat dilihat dari proses pengujiannya dimana peneliti melakukan pengujian terhadap data yang dikirim dan data yang diterima seperti pengujian *troughput, packet loss* dengan beban *Iperf* yang berbeda dengan jaringan non-SDN dana jaringan menggunakan SDN sehingga dapat diketahui pada penelitian tersebut penggunaan jaringan tidak meliputi penambahan security untuk meningkatkan keamanaan jaringan tersebut. Selanjutnya pada penelitian yang dilakukan oleh Fatimah Abdulnabi Salman

dengan judul "Implementation of IPsec-VPN Tunneling using GNS3". Pada penelitian ini peneliti tersebut menggunakan jaringan VPN dengan penambahan keamanan IPSec menggunakan GNS3. Desain yang digunakan pada penelitian ini menggunakan 2 client topology dan digunakan sebagai bahan pengujian yaitu melakukan request ping untuk mengetahui proses paket yang terjadi selain itu juga menggunakan tambahan wireshark untuk mengetahui bahwa data yang direquest oleh client terenskrip dengan identify protection sehingga pada client yang telah diatur memiliki fasilitas keamanan dengan mengenskrip data antara client dan server menggunakan jaringan VPN. Selanjutnya penelitian yang telah dilakukan oleh Maryanto, dkk, dengan judul "Metode *Internet Protocol Security (IPSec)* Dengan *Virtual Private Network (VPN)* Untuk Komunikasi Data" dimana penelitian ini juga menggunakan jaringan VPN dengan *tunneling IPSec* sehingga memiliki jaringan dengan fasilitas keamanan. Pada pembuatannya ada beberapa tahap yang terjadi seperti pengaturan firewall untuk salah satu proses security, ada pengaturan tunnel interface untuk menentukan jalur tunnel daringan internet ke jaringan yang terkoneksi internet dan pengaturan IPSec untuk menentukan jalur tunnel yang telah dibuat. Pada pengujian yang dilakukan peneliti tersebut yaitu mengirim request ping untuk mengetahui proses packet yang terjadi dan paket data yang telah dikirim berhasil dienskrip atau tidaknya tetapi pada penelitian ini digunakan pada jaringan VPN.

Pada 3 penelitian sebelumnya terdapat salah satu peneliti menggunakan jaringan SDN dimana hasil yang diperoleh hanya membandingkan saja antara penggunaan jaringan non-SDN dan jaringan dengan SDN dengan beban yang berbeda sehingga tidak memiliki fasilitas keamanan pada jaringan tersebut.

Sedangkan pada 2 penilitan yang telah dijabarkan diatas menggunakan jaringan VPN tetapi memiliki fasilitas keamanan yang sama yaitu menggunakan *Internet Protocol-Security (IPSec)* sebagai metode untuk mengenskrip data yang dikirim pada jaringan tersebut dengan jenis topology yang berbeda sesuai dengan desain dan kebutuhan.